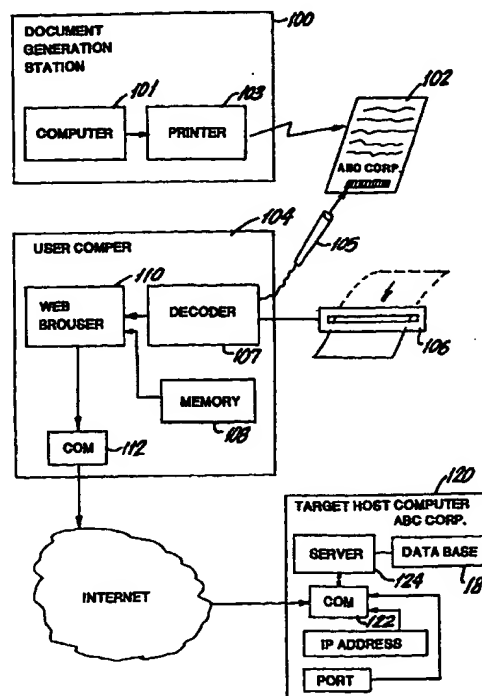# PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:	**WO 98/38761**
H04L	A2	(43) International Publication Date:	3 September 1998 (03.09.98)

(21) International Application Number: PCT/US98/02716

(22) International Filing Date: 13 February 1998 (13.02.98)

(30) Priority Data:
60/037,988   13 February 1997 (13.02.97)   US

(71) Applicant *(for all designated States except US)*: NEOMEDIA TECHNOLOGIES, INC. [US/US]; Suite 600, 2201 Second Street, Fort Myers, FL 33901 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: DURST, Robert, T., Jr. [US/US]; 6054 Timberwoods Circle #240, Fort Myers, FL 33908 (US).

(74) Agent: TURNER, Roderick, S., W.; Suite 200, 14 South Main Street, Sayville, NY 11782 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: AUTOMATIC SERVER ACCESS IN AN INTERNETWORKED COMPUTER SYSTEM

(57) Abstract

The present invention provides a method for encoding a host Internet Protocol (IP) address within a linear (i.e. one dimensional) barcode which enables a direct link to a designated host computer without third party intervention. Additional information may be made available to the designated host or other parties directly or through a commercial server which include but are not limited to client demographics and usage, and data regarding the publication within which the barcode was discovered by the client. The present invention also contemplates a method which restricts access to only those server addresses which exhibit authorized and licensed codes validated and analyzed by a process resident on the client computer. The present invention pertains to both "open" and "closed" Internet implementations such as TCP/IP and client/server environments (e.g. World Wide Web and html). The invention may be adapted to a wide variety of software and hardware applications available to the typical client such as personal computers equipped with appropriate communications and session software, workstations, dedicated network computers, handheld terminals, and web-ready television.

AUTOMATIC SERVER ACCESS IN AN INTERNETWORKED COMPUTER SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

This application is based on and claims the priority of

5   co-pending provisional patent application filed in the

United States Patent and Trademark Office on February 13,

1997 and assigned Serial No. 60/037,988.

TECHNICAL FIELD

10   This invention relates to the Internet, and in

particular to a method for encoding a host Internet Protocol

(IP) address within a linear (i.e. one dimensional) barcode

which enables a direct link to a designated host computer

without third party intervention

15

BACKGROUND ART

Electronic data sources, such as conventional

databases, the Internet and the World Wide Web (WWW) are a

rich and important means of information retrieval and

20   distribution and, increasingly, electronic commerce.

However, there are problems finding the information desired

in this increasingly complex and changing network of data

sources. Recently introduced Internet "search engines",

such as Yahoo, help by allowing a user to search on-line

25   indices of information sources, and even full source text,

for relevant key words and phrases related to their topic of

interest, but even carefully structured queries by

experienced users often results in hundreds and even

thousands of possible "hits" which are not sufficiently

1

specific to preclude further manual search which is both
data resource inefficient and time consuming.

Because of these inefficiencies, as well as general
lack of familiarity with search engines and their syntax,
users are often rely on human readable print and broadcast
media advertising to identify source addresses (e.g.,
Uniform Resource Locators ("URLs")) for web sites and other
online information of interest. Print media is particularly
effective since: (1) it is the most ubiquitous method of
communication and advertising in the modern world; and (2) a
printed document can serve as a persistent reference to be
saved and used during a subsequent on-line session or
sessions.

However, human readable printed source addresses, and
especially URL's, are particularly difficult to manually
enter in software programs, such as "web browsers", due to
their length and use of complex and unfamiliar symbols. If
the characters in an address are not entered exactly,
retrieval is prevented or, in a limited number of cases, a
legal but incorrect source is accessed. This is especially
true when URLs incorporate foreign languages and/or complex
query instructions to on-line databases, as is increasingly
frequent in most web sites. In addition, the inability to
type or otherwise manually enter symbolic address
information due to either disability or lack of training
complicates use of on-line information resources such as the
Internet and World Wide Web for millions of individuals.

Finally, it is widely anticipated that Internet and WWW
access will increasingly be provided through interactive
cable television via web-ready television receivers and set-
top boxes used in conjunction with conventional television
5   receivers. In this home "entertainment" environment, it is
difficult to use keyboards for address entry due to both
lack of typing skill and the cumbersome placement of these
components. Another method which would eliminate typing and
allow users to directly link printed addresses and query
10   scripts to electronic information sources would be highly
desirable.

Information is currently distributed in print (i.e.
hardcopy) and electronic means (i.e. softcopy). While both
15   methods originate from computers each provides a different
set of advantages as well as shortcomings.

Printed documents continue to provide the most
ubiquitous media and in fact the primary basis for legal,
20   commercial, and educational applications. However, the use
of electronic media is expanding rapidly in the fields of
multimedia and interactive applications. Printed documents
are subject to inaccuracies created by the loss of
synchronization with the original source of data. In
25   addition, when compared with multimedia and interactive
applications, printed matter is somewhat limited in its
ability to provide an effective means of presentation to the
potential reader. Conversely, information in electronic
format is often not readily available and requires computer
30   mediation.

Therefore, in order to overcome the disadvantages of either source of information while enhancing each of their inherent advantages it would be highly beneficial to be able

5   to link printed documents to electronic resources. This is not intended as a limitation to on-line and Internet resources, since printed documents could also be linked to storage on local media within a local or distributed system.

10   By linking the two forms of information printed material could be augmented, enhanced and verified through electronic resources. Another benefit to be derived is found in expediting the efficient retrieval of data. The value of this benefit is shown in the widespread acceptance

15   of WWW addresses which have been incorporated into printed documents.

As discussed above entry of WWW addresses is often cumbersome since exact human data entry of complex and

20   unfamiliar strings of text is often required. Also, commercial enterprises are excluded from obtaining valuable demographics concerning those consumers seeking information at the commercial Internet address or for that matter the printed matter which provided the Internet address to the

25   consumer.

One potential solution to this problem is to render the URL address in the form of a machine readable code such as barcodes (linear or two dimensional) or via Optical

30   Character Recognition (OCR) techniques. The barcode could

4

be scanned with a dedicated or general purpose device equipped to decode the URL address and link the user to the correct URL address using appropriate applications software. However, the disadvantages of these method are that OCR

5 techniques are not reliable for decoding all characters in the various fonts found in printed material. In addition, although two dimensional barcodes are capable of encoding lengthy strings of information, cost effective hardware and software for decoding two dimensional barcodes are not

10 readily available at this time. Also, conventional linear barcodes have insufficient capacity to render character based URL addresses in a practical manner within an efficient amount of space.

15 Therefore, there is a need for a method which links printed material with electronic resources that is capable of providing access to the link via readily available and cost effective hardware and software.

20 ## DISCLOSURE OF THE INVENTION

The present invention provides a method for encoding a host Internet Protocol (IP) address within a linear (i.e. one dimensional) barcode which enables a direct link to a designated host computer via the Internet without third

25 party intervention. Additional information may be made available to the designated host or other parties directly or through a commercial server which include but are not limited to client demographics and usage, and data regarding the publication from which the bar code was discovered by

30 the client. The present invention also contemplates a

method which restricts access to only those server addresses which exhibit authorized and licensed codes validated and analyzed by a process resident on the client computer. The present invention pertains to both "open" and "closed" Internet and Intranet implementations such as TCP/IP and client/server environments (e.g. World Wide Web and html). The invention may be adapted to a wide variety of software and hardware applications available to the typical client such as personal computers equipped with appropriate communications and session software, workstations, dedicated network computers, handheld terminals, and web-ready television.

In particular, the present invention provides a method for automatically linking a client or user computer with a target server or host computer for data transmission therebetween, said method comprising the steps of:

a) assembling a data string comprising a network address of the target server computer and a target file index pointer;

b) encrypting the data string utilizing an encryption key;

c) generating a printed document comprising a machine readable symbol, the machine readable symbol comprising said encrypted data string;

d) scanning the machine readable symbol with scanning means coupled with the client computer to produce scanned data;

6

e) decrypting the scanned data with a key stored on said client computer and associated with the encryption key;

f) processing the decrypted data to decode the target server computer network address and target file pointer;

g) assembling a data message for transmission over the computer network, the data message comprising the target file pointer and user-specific data from a memory associated with the client computer, the data message being prepended with the target server computer network address in accordance with a transmission protocol associated with the computer network;

h) transmitting the data message over the computer network;

i) receiving the data message at the target server computer;

j) unpacking the data message to determine the target file pointer;

k) retrieving from memory a target file associated with the target file pointer;

i) assembling a return data message for transmission over the computer network, the return data message comprising the target file and being prepended with a computer network address associated with the client computer;

l) transmitting the return data message over the computer network; and

m) receiving the return data message at the client computer.

BRIEF DESCRIPTION OF THE DRAWING

These and other objects and features of the
invention shall now be described in relation to the
drawings:

5

Figure 1 is a flowchart illustrating the method of the
present invention.

Figure 2 is a block diagram of the system of the
present invention.

10   Figure 3 is an illustration of the data format for
encoding into a bar code.

Figure 4 is an alternative block diagram of the present
invention.

15   ## BEST MODE FOR CARRYING OUT THE INVENTION

A document 102 embedded with an Internet hot-link bar-
code is generated by a document generation station 100 as
shown in Figure 2. The document generation station 100
comprises a general purpose computer 101, which may be a
20   personal computer, dedicated printer computer, or the like.
Attached thereto in customary fashion is a document printer
103. The general purpose computer 101 is programmed with
software that carries out the function to be described
herein for generating the embedded document 102, i.e.,
25   memory and bar code encoding.

The first step of the process takes place in the
document generation station 100 which controls the
formatting of a code symbology such as a linear bar code to
30   be printed onto the document 102. Prior to printing the bar

8

code on the printed document 102, a host Internet Protocol

(IP) address related to the target server 124 (the software

which runs on the host computer that will be linked by

scanning the document) is designated following standard

5   TCP/IP syntax and a specific port is identified in step 1 of

Figure 1 if a default port for the host computer 120 has not

been assigned. Similarly, process values representing

publication information and predetermined responses to be

returned by the target server 124 are defined in step 2.

10   Both sets of information are expressed as binary strings in

a predefined format in step 3 suitable for later parsing

(e.g. data compression). An example of the binary string

format is shown in Figure 3.

15   The following excerpts from the text entitled "Computer

Networks and Internets" by Douglas E. Comer are included in

order to provide further details regarding the IP address:

            In the TCP/IP protocol stack, addressing is

20   specified by the Internet Protocol (IP). The IP

            standard specifies that each host is assigned a

            unique 32-bit number known as the host's Internet

            Protocol address which is often abbreviated IP

            address, or Internet address. Each packet sent

25   across the Internet contains the 32-bit IP address

            of the sender (source) as well as the intended

            recipient (destination). Thus, to transmit

            information across a TCP/IP Internet, a computer

            must know the IP address of the remote computer to

30   which the information is being sent.

Conceptually, each 32-bit IP address is
divided into two parts: a prefix and suffix; the
two-level hierarchy is designed to make routing

5   efficient. The address prefix identifies the
physical network to which the computer is
attached, while the suffix identifies an
individual computer on that network. That is,
each physical network in the Internet is assigned

10   a unique value known as a network number. The
network number appears as a prefix in the address
of each computer attached to the network.
Furthermore, each computer on a given physical
network is assigned a unique address suffix.

15   Although no two networks can be assigned the same
network number and no two computers on the same
network can be assigned the same suffix a suffix
value can be used for more than one network. The
IP address hierarchy guarantees two important

20   properties:

        1. Each computer is assigned a unique address
           (i.e. a single address is never assigned
           to more than one computer).

25

        2. Although network number assignments must
           be coordinated globally, suffixes can be
           assigned locally without global
           coordination.

30

The first property is guaranteed because a
full address contains both a prefix and a suffix,
which are assigned to ensure uniqueness. If two
computers are attached to different physical
5   networks, their addresses have different prefixes.
If two computers are attached to the same physical
network, their addresses have different suffixes.

Once they chose a size for IP addresses and
10   decided to divide each address into two parts, the
designers of IP had to determine how many bits to
place in each part. The prefix needs sufficient
bits to allow a unique network number to be
assigned to each physical network in the Internet.
15   The suffix needs sufficient bits to permit each
computer attached to a network to be assigned a
unique suffix. No simple choice was possible
because adding bits to one part means subtracting
bits from the other. Choosing a large prefix
20   accommodates many networks, but limits the size of
each network; choosing a large suffix means each
physical network can contain many computers, but
limits the total number of networks.

25   Thus, the data to be included in the bar code to be
printed in the document 102, as shown in Figure 3, includes
the target server IP address in the aa.bb.cc.dd format, the
(optional) port number, and data to indicate to the target
server 124 which file should be sent back to the user
30   computer 104. For example, if a hot-link bar code is

printed on a stock prospectus for ABC Corporation, then the
server file ID might point to a file on the server that will
return data relevant to the financial position of ABC
Corporation. Similarly, a hot-link bar code for ABC

5   Corporation that is printed as a product brochure might
return a file related to the specification of that product.

Optionally, the server file ID field may be omitted,
which will allow a smaller bar code symbol to be utilized.

10   In this case, the target server computer will return a file
found at a default location.

The resulting binary string or token is then encrypted,
obfuscated (rendered obscure through a cipher or other non-

15   encryption technique) and optionally signed with an
encryption key in step 4 of Figure 1, all of which may be
accomplished through techniques well known in the art.
Alternatively, a hashing function could be performed upon
the token and the result used as a digital signature

20   appended to the printed document. The proper decryption,
de-obfuscation or signature verification is subsequently
performed by the user's computer decoding software to
confirm that a licensed party generated the token. The
token is then converted to an ASCII string in step 5 which

25   is then converted to the standard syntax of a machine
readable code in step 6 such as OCR text, a linear barcode,
a two dimensional barcode (e.g. PDF417 as discussed in
detail in United States Patent Number 5,399,846 which is
hereby incorporated by reference) or Magnetic Ink Character

30   Recognition (MICR) encoding. The machine readable code is

then rendered as a component of the printed document 102 in step 7. The printed document 102 is then ready for distribution and circulation.

The next step of the process takes place in the user's computer 104 which is equipped with a bar code scanning device, such as a wand 105, which is adapted to scan the machine readable code in accordance with techniques well known in the art. The user computer 104 then decodes the data from the wand 105 via a decoder 107, and utilizes a stored decryption key to decrypt the data and verify its authenticity. A reading means in addition to the wand 105 may be chosen from any number of devices equipped to interface with peripherals capable of reading bar codes. In order to retrieve indexed information from the bar code, the bar code is scanned in step 8, either specifically by the wand 105 or in the process of digitally scanning the entire document via an optional page scanner 106.

The decoded ASCII string is then converted to a corresponding binary equivalent in step 9 and is decrypted, de-obfuscated or the signature of the string or its hash is verified to confirm generation by an authorized or licensed party in step 10 which results in a token. If the token thus derived is not valid as determined in step 10 the retrieval process is terminated in step 12.

However, if the token is valid, it is expanded to reconstruct the IP address and port, document and process values in step 13 which are required to retrieve the indexed

information from the target server. Usage and demographic
information descriptive of the user computer 104 may
optionally be retrieved from memory 108 and encrypted,
obfuscated and signed in step 22 using a key 25 provided by
a licensing party. The information resulting from step 21
is associated with the extracted IP address and port,
document and process values from step 13, and then formatted
using the syntax appropriate for an Internet communication
session (e.g. WWW, html) thereby enabling a query to be
asserted in step 14.

The query is transmitted onto the Internet by the
user's web browser 110 in conjunction with an Internet
communication module 112. After being routed to the target
host computer 120 via standard Internet techniques, the
query is unpacked and parsed by a communication module 122
and server 124 in step 15.

The target host computer 120 then activates the server
file 124 which fetches the requested information from
storage or generate the requested information using
programmed retrieval and formatting processes (e.g. CGI,
RDBM) in step 16. In one embodiment static preformatted
information (e.g. html), RDBMS elements and CGI and RDBMS
scripts are stored on a local host database 18, however,
such information could also be stored on an appropriate
device accessible through structured data communications
with the host including the client. These transactions can
also be logged in step 17 for subsequent analysis concerning
traffic and reconciliation with licensing charges. The

retrieved or generated information is then formatted for
transmission to the user computer 104 and transmitted using
appropriate protocols (e.g. TCP/IP) in step 19. This
information is then displayed to the user on the user

5   computer 104 and a screen dialog between the user and the
information system proceeds. A portion of the content or
format of the information presented to the user could be
tailored to the individual user based on demographic and
usage information conveyed in the original query.

10

       Alternatively, the query information, particularly the
demographic and usage information, may be stored in the form
of an activity log in step 23 on a separate server or as an
activity database 24 on the host computer 120. In the case

15   where the activity database 24 is stored on the host
computer 120 the activity database 24 is encrypted and the
information is retrieved for marketing or some other purpose
in step 26, and decrypted in step 27 using the access key 25
which would generally be under the control of the licensing

20   party and provided under commercial licensing terms.
Following decryption this information could then be
displayed or printed in step 29 or stored in step 28 for
future analysis and use by the licensed publisher or vendor.

25   The classes of user computer devices that ay be used
with the present invention include, but are not limited to,
general purpose personal computers, workstations, handheld
computers such as Personal Digital Assistants (PDA), network
computers, intelligent display telephones (e.g. the "smart

30   phone" commercially available through Phillips

15

Corporation),data communications capable set top boxes, or
television receivers with integrated data communications
capability (i.e. web-ready television).

CLAIMS:

1. In computer network comprising a user client computer and a target server computer, a method for
5   automatically transferring a target data file from the target server computer to the client computer, said method comprising the steps of:

a) assembling a data string comprising a network address of said target server computer and a target file
10   index pointer, said target file index pointer associated with said target data file to be transferred from said target server computer;

b) encrypting said data string utilizing an encryption key;

15   c) generating a printed document comprising a machine readable symbol, said machine readable symbol being encoded with said encrypted data string;

d) scanning said machine readable symbol with scanning means coupled to said client computer to produce a scanned
20   data string;

e) producing a decrypted data string by decrypting said scanned data string with a key stored on said client computer and associated with said encryption key;

f) processing said decrypted data string to decode said
25   target server computer network address and target file index pointer;

g) assembling a data request message for transmission over the computer network, said data message comprising said target file index pointer and user-specific data from a
30   memory associated with said client computer, said data

17

request message being prepended with said target server
computer network address in accordance with a transmission
protocol associated with said computer network;

5   h) transmitting said data request message over said
computer network;

i) receiving said data request message at said target
server computer;

j) unpacking said data request message to determine
said target file index pointer;

10   k) retrieving from memory said target file associated
with said target file index pointer;

i) assembling a data return message for transmission
over the computer network, said data return message
comprising said target file and being prepended with a
15   computer network address associated with said client
computer;

l) transmitting said data return message over the
computer network; and

m) receiving said data return message at said client
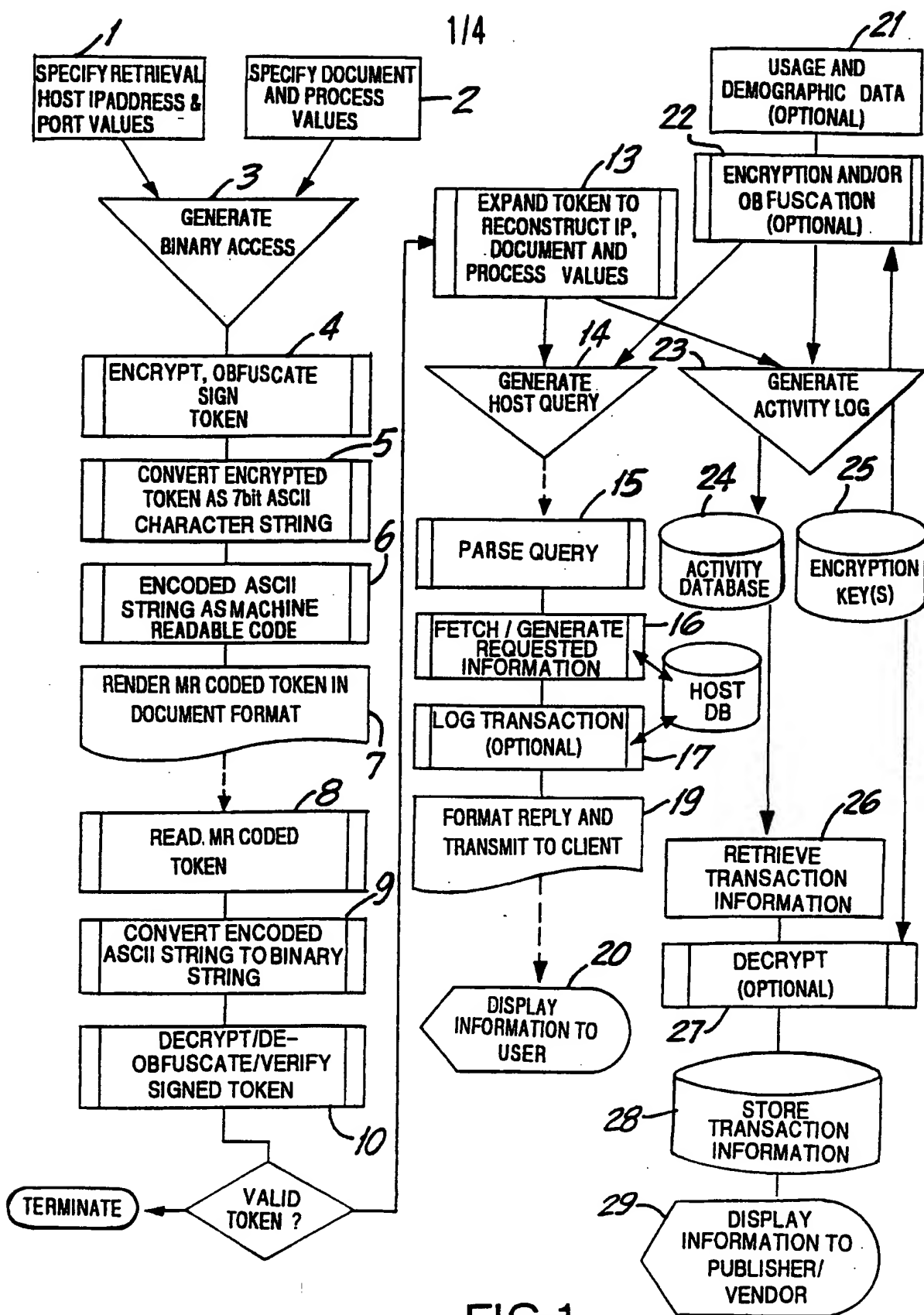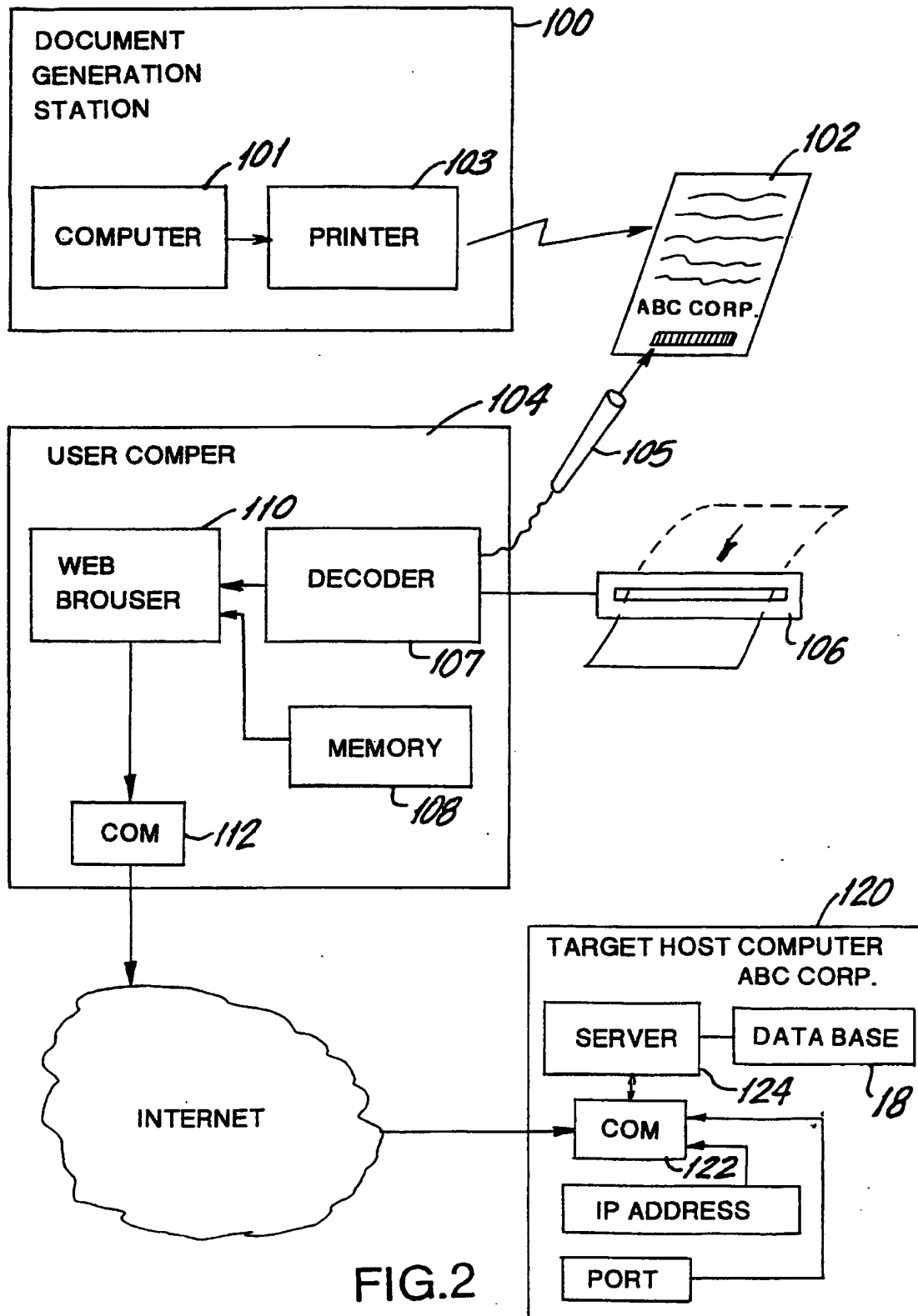20   computer.

FIG.1

2/4

FIG.2

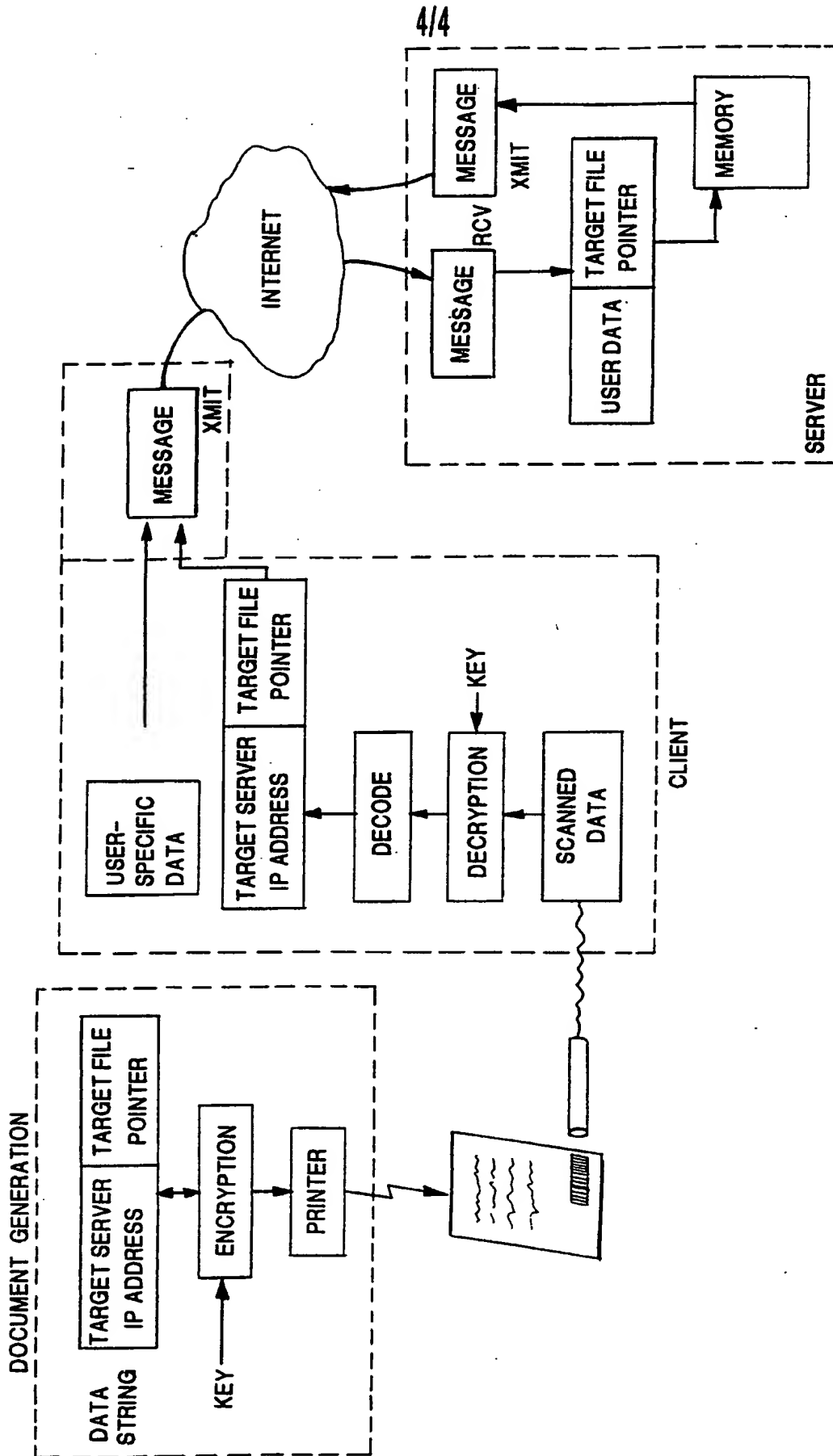| TARGET SERVER IP ADDRESS (aa.bb.cc.dd.)	PORT	SERVER FILE ID

FIG.3

4/4

FIG.4